EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Larry Galvin on 03/14/2008.

The claims have been amended as follows:

2. In claim 1, replace line 19 with, “an S-register in which a bit value s_i of the sum S is updated and stored; and"

3. In claim 1, replace line 20 with, “a C-register in which a bit value c_i of the carry C is updated and stored.”

4. In claim 18, replace line 16 with “an S-register in which a bit value s_i of the sum S is updated and stored; and"

5. In claim 18, replace line 17 with “a C-register in which a bit value c_i of the carry C is updated and stored;”

6. In claim 18, replace lines 1-2 with, "A system embodying a Montgomery modular multiplier <u>of a public-key cryptographic system</u>, the system comprising:

7. Claims 19-20 cancelled.

8. In claim 21, line 2, replace -a public key- with "the public-key"

REASONS FOR ALLOWANCE

9. Claims 1-15 and 17-22 are allowed.

10. The following is an examiner's statement of reasons for allowance:

11. The prior art of record fails to teach or suggest the claimed invention. Specifically the prior art of record fails to teach or suggest the Montgomery modular multiplier structure having at least a q_i calculation logic circuit solving a Boolean logic equation "s_0 XOR c_0 XOR (b_i AND a_0)," and a compressor performing n additions on the carry C, the sum S, the b_iA, and the q_iM to obtain interim values and summing the interim values to obtain a result using a carry propagation adder in response to a carry propagation adder signal, as recited in independent claims 1, 7, 17, and 18.

12. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL YAARY whose telephone number is (571)270-1249. The examiner can normally be reached on Monday-Friday, 8:00 a.m - 5:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lewis Bullock can be reached on (571) 272-3759. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. Y./
Examiner, Art Unit 2193

/Lewis A. Bullock, Jr./
Supervisory Patent Examiner, Art Unit 2193